In the Claims

Please cancel, without prejudice to Applicant's right to pursue the claims in a continuation application (and/or continuation-in-part), Claims 6, 7, 9, 11-14, 18, 20, 21 and 30. Applicant reserves the right to pursue the subject matter of the original claims in this application and in other applications.

The November 19, 2008 Office Action Summary states that "Claims 1-31 is/are pending in the application." Clarification is respectfully sought as the previous Office Action[s] indicate Claims 6-21, 30 and 31 are pending in the instant application.

Please amend Claims 8, 10, 15-17, 19 and 31 as directed by the Office Action of November 19, 2008 under the heading "Allowable Subject Matter", that "... Claims 8, 10, 15-17, 19 and 31 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims" (Page 2). Applicant confirmed these express instructions during the Interview on or about December 10, 2008 with Supervisory Examiner Barron and Examiner Okeke. *Please see* 37 CFR § 1.111. As well, *please see*, MPEP § 701.01 & MPEP § 608.01(n).

The following amendments rely upon additional confirmation of the Examiners' instructions in the Interview Summary of December 17, 2008. Applicant presents arguments for the rejected claim[s] as agreed during the Interview, in the interests of compact prosecution (MPEP § 2106) and Office standard for determination of patentability based on the entire record, a preponderance of evidence, with due consideration to the persuasiveness of any arguments and secondary evidence. *In re Oetiker*, 977 F.2d 1443 (Fed. Cir. 1992). *Please see*, *Zurko, In re Lee* and in *Gartside*.

Listing of Claims:

Claims 1 - 7 (canceled without prejudice or disclaimer)

8. (currently amended) [[The method of claim 6,]] A method for protecting a digital signal, comprising the steps of:

providing a digital signal comprising digital data and file format information defining how the digital signal is encoded;

creating a predetermined key to manipulate the digital signal wherein the predetermined key comprises a plurality of mask sets[[.]]; and

manipulating the digital signal using the predetermined key to generate at least one permutation of the digital signal parameterized by the file format information defining how the digital signal is encoded.

Claim 9 (canceled without prejudice or disclaimer)

10. (currently amended) [[The method of claim 6,]] A method for protecting a digital signal, comprising the steps of:

providing a digital signal comprising digital data and file format information defining how the digital signal is encoded;

creating a predetermined key to manipulate the digital signal wherein the predetermined key comprises a key pair comprising a public key and a private key[[.]]; and

manipulating the digital signal using the predetermined key to generate at least one permutation of the digital signal parameterized by the file format information defining how the digital signal is encoded.

Claims 11 - 14 (canceled without prejudice or disclaimer)

15. (currently amended) [[The method of claim 6,]] A method for protecting a digital signal, comprising the steps of:

providing a digital signal comprising digital data and file format information defining how the digital signal is encoded;

creating a predetermined key to manipulate the digital signal wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the steps of:

generating a hash value using the one or more masks sets; and

authenticating the one or more mask sets by comparing the generated hash value with a predetermined hash value[[.]]; and

manipulating the digital signal using the predetermined key to generate at least one permutation of the digital signal parameterized by the file format information defining how the digital signal is encoded.

16. (currently amended) [[The method of claim 13,]] A method for protecting a digital signal, comprising the steps of:

providing a digital signal comprising digital data and file format information defining how the digital signal is encoded;

creating a predetermined key to manipulate the digital signal wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the step of:

validating the one or more mask sets before manipulating the file format information using the predetermined key.

wherein said step of validating comprises the steps of:

generating a digital signature using the one or more mask sets; and

comparing the digital signature with a predetermined digital signature[[.]]; and

manipulating the digital signal using the predetermined key to generate at least one permutation of the digital signal parameterized by the file format information defining how the digital signal is encoded.

17. (currently amended) [[The method of claim 6,]] A method for protecting a digital signal, comprising the steps of:

providing a digital signal comprising digital data and file format information defining how the digital signal is encoded;

creating a predetermined key to manipulate the digital signal wherein the predetermined key comprises one or more mask sets having random or pseudo-random series of bits, the method further comprising the step of:

authenticating the one or more mask sets by comparing a generated digital signature with a predetermined digital signature[[.]]; and

manipulating the digital signal using the predetermined key to generate at least one permutation of the digital signal parameterized by the file format information defining how the digital signal is encoded.

Claim 18 (cancelled without prejudice or disclaimer)

19. (currently amended) [[The method of claim 6,]] A method for protecting a digital signal, comprising the steps of:

providing a digital signal comprising digital data and file format information defining how the digital signal is encoded;

creating a predetermined key to manipulate the digital signal further comprising the step of:

computing a secure one way hash function of data in the digital signal, wherein the secure one way hash function is insensitive to changes introduced into the digital signal during the step of file format manipulation[[.]] and;

manipulating the digital signal using the predetermined key to generate at least one permutation of the digital signal parameterized by the file format information defining how the digital signal is encoded.

Claims 20 - 30 (cancelled without prejudice or disclaimer)

31. (currently amended) [[The method of claim 30,]] A method for protecting digital data, where the digital data is organized into a plurality of frames, each frame having i) a header comprising file format information and ii) at least a portion of the digital data, said method comprising the steps of:

creating a predetermined key to manipulate the file format information in one or more of the plurality of frames wherein the file format information defines how the digital data is encoded wherein the predetermined key comprises a private key that is associated with a key pair [[.]]; and

manipulating the file format information using the predetermined key in at least two of the plurality of frames wherein the file format information defines how the digital data is encoded, such that the digital data will be perceived by a human as noticeably altered if it is played without using a decode key to restore the file format information to a prior state.